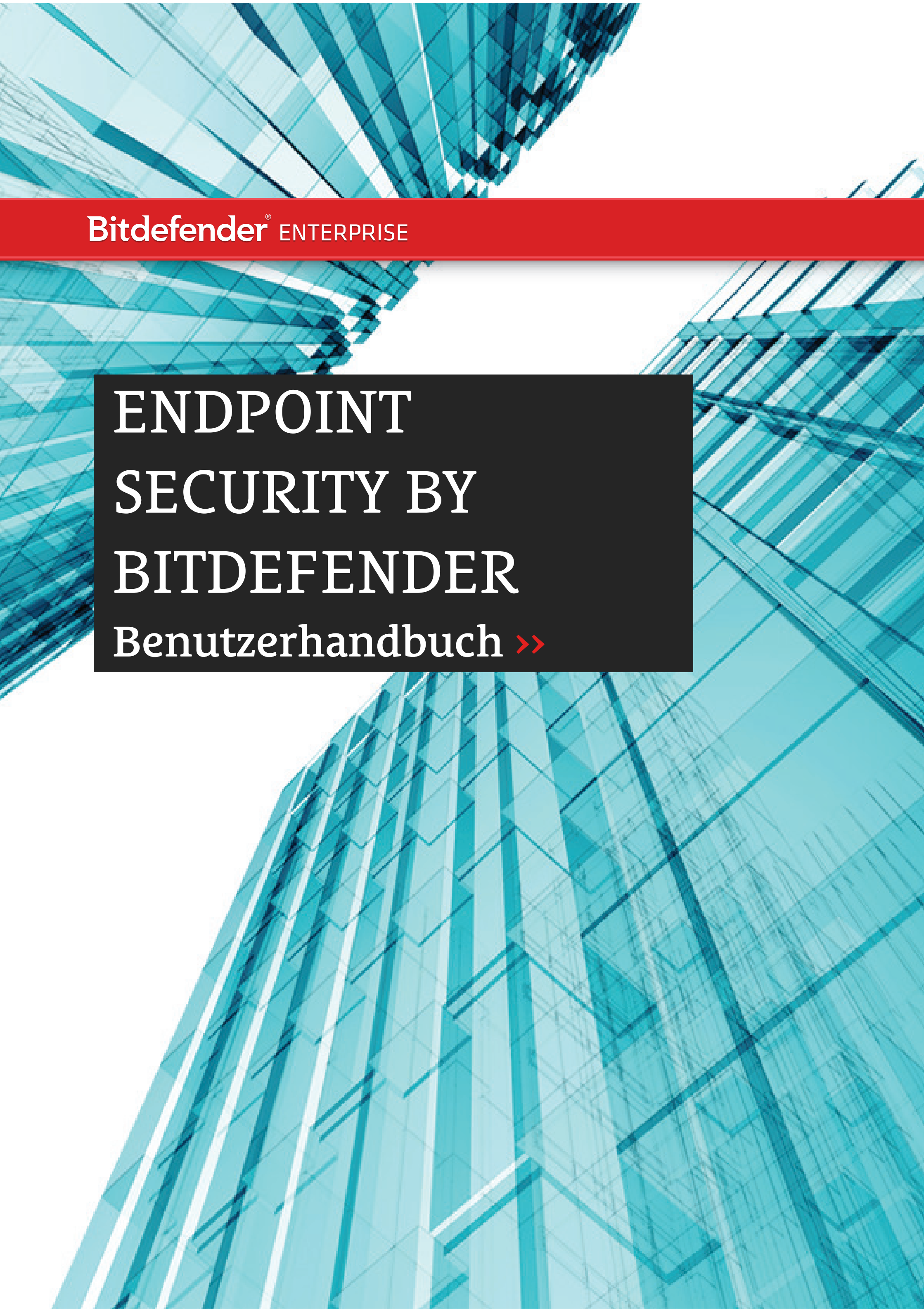


ENDPOINT SECURITY BY BITDEFENDER

Benutzerhandbuch ››

Veröffentlicht 2014.09.30


Bitdefender®

Inhaltsverzeichnis

Zur Verwendung dieses Handbuchs

1. Zielsetzung und Zielgruppe

Diese Dokumentation richtet sich an die Endanwender von **Endpoint Security**, der Security for Endpoints-Client-Software, die auf Computern und Servern installiert wird, um diese vor Malware und anderen Bedrohungen aus dem Internet zu schützen und die Einhaltung von Richtlinien für die Benutzerkontrolle sicherzustellen.

Die hier bereitgestellten Informationen sollten für jeden Benutzer mit Erfahrung im Umgang mit Windows verständlich sein.

Viel Spaß mit diesen nützlichen und informativen Handbuch.

2. Über dieses Handbuch

Dieses Handbuch ist übersichtlich gestaltet, damit Sie im Handumdrehen alle benötigten Informationen finden können.

„Erste Schritte“ (S. 1)
Machen Sie sich mit der Endpoint Security-Benutzeroberfläche vertraut.

„Scannen auf Malware“ (S. 9)
Erfahren Sie, wie Sie Malware-Scans ausführen können.

„Updates“ (S. 17)
Erfahren Sie mehr über Endpoint Security-Updates.

„Ereignisanzeige“ (S. 19)
Überprüfen Sie die Aktivität von Endpoint Security.

„Hilfe erhalten“ (S. 20)
Beschreibt wie Sie Hilfe bzw. Unterstützung zu dem Produkt erhalten und erhält zusätzlich eine Liste mit den am häufigsten gestellten Fragen (FAQ).

3. Konventionen in diesem Handbuch

Typografie

Um die Lesbarkeit zu fördern werden verschiedene Arten von Textstilen verwendet. Die jeweiligen Bedeutungen entnehmen Sie bitte der nachfolgenden Tabelle.

Erscheinungsbild	Beschreibung
documentation@bitdefender.com	Verweise auf E-Mail-Adressen, z.B. zur Kontaktaufnahme.
„Zur Verwendung dieses Handbuchs“ (S. v)	Interne Verweise (Links) auf beliebige Stellen innerhalb dieses Dokuments.
`Dateiname`	Dateien und Verzeichnisse werden in einer Schriftart mit `fester Laufweite` angegeben.
Option	Alle Produktoptionen werden **fett gedruckt** dargestellt.
Stichwort	Wichtige Stichwörter oder Begriffe werden durch **Fettdruck** hervorgehoben.

Symbole

Bei diesen Symbolen handelt es sich um Hinweise innerhalb des Textflusses welche mit einer kleinen Grafik markiert sind. Hierbei handelt es sich um Informationen die Sie in jedem Fall beachten sollten.



Beachten Sie

Diese Bemerkung dient lediglich zur Überprüfung. Notizen enthalten nützliche Informationen wie zum Beispiel einen Verweis auf ein verwandtes Thema.



Wichtig

Diese Art von Hinweis sollte in jedem Fall gelesen werden. Es werden signifikante Informationen zum jeweiligen Thema bereitgestellt. Es wird nicht empfohlen diese zu übergehen.

4. Ihre Mithilfe

Wir laden Sie ein mit zu helfen unser Buch zu verbessern. Wir haben sämtliche Informationen in diesem Dokument bestmöglich überprüft um somit die Qualität sicherzustellen. Bitte schreiben Sie uns bezüglich Fehler, die in diesem Buch finden oder auch bezüglich Dinge, die Ihrer Meinung nach verbessert werden könnten. Dies hilft uns Ihnen die beste mögliche Dokumentation zur Verfügung zu stellen.

Falls Sie dennoch Fehler finden, so teilen Sie uns diese bitte mit indem Sie uns per E-Mail unter der Adresse documentation@bitdefender.com kontaktieren. Bitte verfassen Sie bitte alle auf die Dokumentation bezogenen E-Mails auf Englisch.

1. Erste Schritte

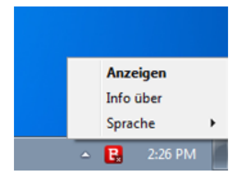
Endpoint Security ist ein vollautomatisches Computer-Sicherheitsprogramm, das von Ihrem Netzwerkadministrator fernverwaltet wird. Nach der Installation schützt sie Sie vor allen Arten von Schad-Software (wie Viren, Spyware und Trojaner), Netzwerkangriffen, Phishing-Versuchen und Datendiebstahl. Zudem kann sie genutzt werden, um die Einhaltung von Richtlinien zur Computer- und Internet-Nutzung sicherzustellen.

Endpoint Security trifft alle sicherheitsrelevanten Entscheidungen für Sie und wird nur in seltenen Fällen Pop-up-Benachrichtigungen anzeigen. Nähere Informationen zu den durchgeführten Aktionen und zur Programmausführung finden Sie im Ereignisfenster. Für weitere Informationen lesen Sie bitte „Ereignisanzeige“ (S. 19).

1.1. Task-Leistensymbol

Nach der Installation wird ein Endpoint Security-Symbol dauerhaft in Ihrer Task-Leiste angezeigt. Bei einem Doppelklick auf dieses Symbol öffnet sich das Hauptenster des Programms. Mit einem Rechtsklick auf das Symbol öffnen Sie ein Kontextmenü mit nützlichen Optionen.

- **Anzeigen** - Öffnet das Endpoint Security-Hauptfenster.
- **Über** - öffnet ein Fenster, in dem Sie Informationen über Endpoint Security erhalten und Hilfe finden, falls etwas Unvorhergesehenes geschieht. Wenn Sie das Fenster öffnen, wird dadurch automatisch ein Bedarf-Update gestartet.
- **Sprache** - hier können Sie die Sprache der Benutzeroberfläche einstellen.

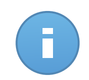


Task-Leistensymbol

Das Endpoint Security-Symbol in der Task-Leiste weist Sie auf Probleme hin, die Ihren Computer beeinträchtigen, indem es sein Aussehen verändert:

Kritische Probleme beeinträchtigen die Sicherheit Ihres Systems.

Nicht-kritische Probleme beeinträchtigen die Sicherheit Ihres Systems.



Beachten Sie

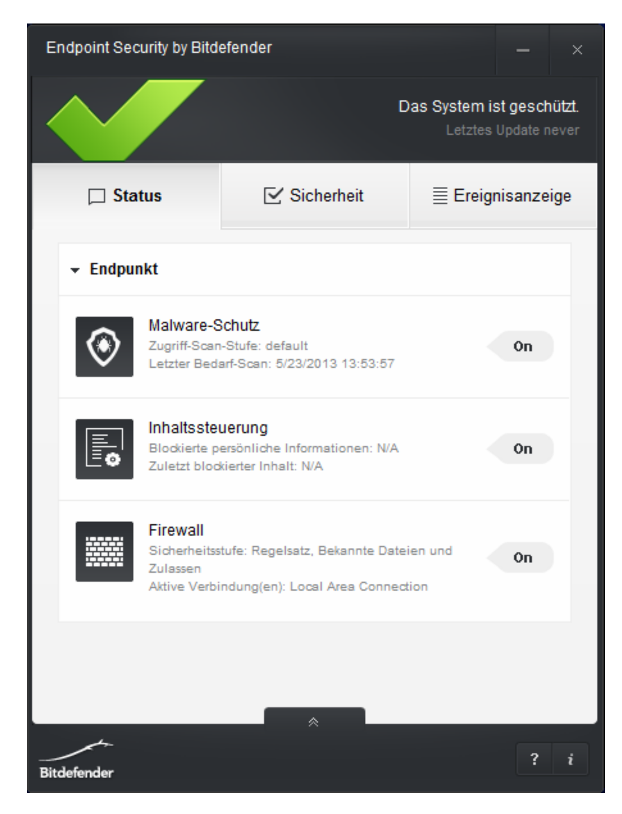
Der Netzwerkadministrator kann das Task-Leistensymbol ausblenden, wenn er möchte.

1.2. Öffnen des Hauptfensters

Sie können die Benutzeroberfläche von Endpoint Security aus dem Windows-Startmenü heraus über den folgenden Pfad aufrufen: **Start** → **Alle Programme** → **Endpoint Security by Bitdefender** → **Sicherheitskonsole öffnen**. Noch schneller geht es mit einem Doppelklick auf das Endpoint Security-Symbol B in der Task-Leiste.

1.3. Hauptfenster

Im Hauptfenster von Endpoint Security können Sie den Sicherheitsstatus überprüfen und Scan-Aufgaben ausführen. Und das alles mit nur wenigen Klicks. Die Konfiguration und Verwaltung der Sicherheit erfolgt per Fernzugriff durch Ihren Netzwerkadministrator.

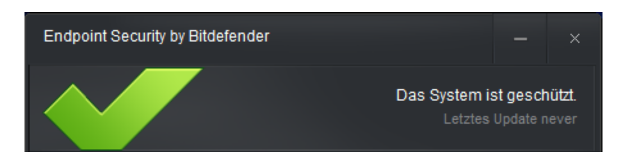


Hauptfenster

Das Fenster ist in zwei Hauptbereiche aufgeteilt:

Infobereich

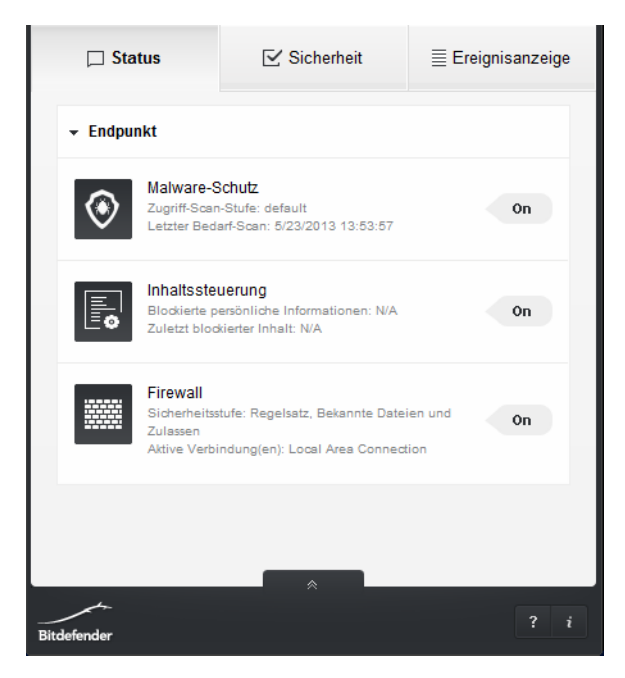
Hier können Sie den Sicherheitsstatus Ihres Computers überprüfen und sehen, welche Probleme die Sicherheit Ihres Systems gefährden.



Infobereich

Tafelbereich

Im Tafelbereich können Sie den Status jedes installierten Sicherheitsmoduls sehen, Bedarf-Scan-Aufgaben verwalten und die von Endpoint Security protokollierten Ereignisse sehen.



Tafelbereich

Zusätzlich finden Sie eine Reihe nützlicher Support-Optionen im unteren Bereich des Fensters:

Optionen	Beschreibung
?	Klicken Sie auf dieses Symbol, wenn Sie Hilfe zu Endpoint Security benötigen.
i	Klicken Sie auf dieses Symbol, um Produkt- und Kontaktinformationen anzuzeigen.

1.3.1. Infobereich

Im Infobereich finden Sie hilfreiche Informationen zur Sicherheit des Systems.

Sie können den aktuellen Sicherheitsstatus ganz leicht am Statussymbol links vom Infobereich ablesen:

- **Grünes Häkchen.** Es müssen keine Probleme behoben werden. Ihr Rechner und Ihre Daten sind geschützt.
- **Gelbes Ausrufezeichen.** Die Sicherheit Ihres Systems wird durch nicht-kritische Probleme beeinträchtigt.
- **Rotes Ausrufezeichen.** Die Sicherheit Ihres Systems wird durch kritische Probleme beeinträchtigt.

Zusätzlich zum Statussymbol wird ein Sicherheitsstatushinweis rechts vom Infobereich angezeigt. Sie können die gefundenen Sicherheitsprobleme anzeigen, indem Sie auf eine beliebige Stelle im Infobereich klicken. Bestehende Probleme werden von Ihrem Netzwerkadministrator behoben.

1.3.2. Tafelbereich

Im Tafelbereich können Sie den Status jedes installierten Sicherheitsmoduls sehen, Bedarf-Scan-Aufgaben verwalten und die von Endpoint Security protokollierten Ereignisse sehen.

In diesem Bereich stehen Ihnen die folgenden Tafeln zur Verfügung:

Status

Hier können Sie Einzelheiten zum Status und der Aktivität der installierten Sicherheitsmodule sehen.

- **Malware-Schutz.** Der Malware-Schutz bildet die Grundlage Ihrer Sicherheit. Endpoint Security schützt Sie sowohl in Echtzeit als auch bei Bedarf vor allen Arten von Malware, so zum Beispiel vor Viren, Trojanern, Spyware, Adware usw.
- **Inhaltssteuerung.** Das Modul Inhaltssteuerung schützt Sie im Internet vor Phishing-Angriffen, Betrugsversuchen, Diebstahl vertraulicher Daten und nicht jugendfreien Inhalten. Darüber hinaus enthält es umfangreiche Benutzersteuerungselemente, mit denen Netzwerkadminstratoren die Einhaltung von Richtlinien zur Computer- und Internet-Nutzung sicherstellen können.

- **Update.** Das Update-Modul stellt sicher, dass Endpoint Security und die Virensignaturen stets auf dem neuesten Stand sind.
- **Firewall.** Die Firewall schützt Sie, wenn Sie mit Netzwerken und dem Internet verbunden sind, indem sie Verbindungsversuche filtert und verdächtigte oder gefährliche Verbindungen blockiert.
- **Allgemein.** In der Kategorie Allgemein finden Sie alle weiteren Details, die in den oben beschriebenen Modulen nicht enthalten sind, so zum Beispiel Informationen zur Produktlizenz.

Sicherheit

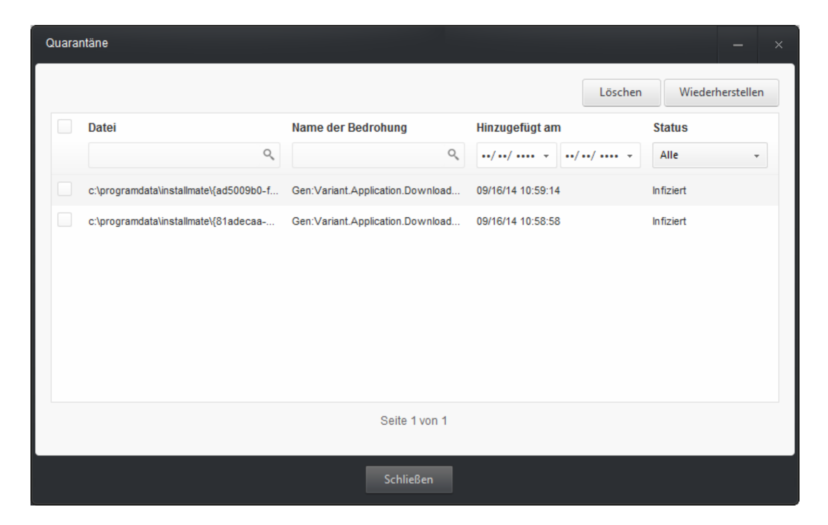
Hier können Sie System-Scans starten. Sie können eine der folgenden Scan-Aufgaben ausführen:

- Beim **Quick Scan** wird das sog In-the-Cloud-Verfahren angewandt, um auf Ihrem System laufende Malware aufzuspüren. Die Ausführung eines Quick Scans dauert im Normalfall weniger als eine Minute und beansprucht nur einen Bruchteil der Systemressourcen, die ein normaler Virenscan in Anspruch nehmen würde.
- Der **Vollständige Scan** durchsucht den gesamten Computer nach allen Typen von Malware, die ein Sicherheitsrisiko darstellen, so z. B. Viren, Spyware, Adware, Rootkits usw.
- **Benutzerdefinierter Scan** Hierbei können Sie die Bereiche, die gescannt werden sollen, selbst auswählen und die Scan-Optionen festlegen.

Weitere Informationen finden Sie unter „Scannen auf Malware“ (S. 9).

Der Bereich **Quarantäne** bietet einen schnellen Überblick über die Anzahl der Dateien, die bei den Scan-Aufgaben in die Quarantäne verschoben wurden.

- Um Dateien in Quarantäne anzuzeigen und entsprechenden Aktionen durchzuführen, klicken Sie auf **Anzeigen**. Die Seite **Quarantäne** wird angezeigt. Hier können Sie eine Liste der Dateien in Quarantäne einschließlich ihres ursprünglichen Speicherorts, Aktionszeit und -datum der Quarantäne sowie Sicherheitsstatus einsehen. Verwenden Sie die Schaltflächen oben rechts, um die gewünschten Dateien zu löschen oder wiederherzustellen.



Quarantäne

- Klicken Sie auf **Leeren**, um alle Dateien in Quarantäne zu löschen.

Ereignisanzeige

Hier können Sie eine detaillierte Übersicht aller relevanten Ereignisse abrufen, die beim Betrieb des Produktes aufgetreten sind. Detaillierte Informationen finden Sie unter „Ereignisanzeige“ (S. 19).

1.4. Surf-Schutz

Ihr Administrator für Security for Endpoints kann Sicherheitseinstellungen vornehmen, die sich auf Ihr Surfen im Internet auswirken. Diese Sicherheitseinstellungen betreffen unter anderem:

- „Bitdefender-Symbolleiste“ (S. 6)
- „Suchberater“ (S. 7)
- „Gesperrte Webseiten“ (S. 7)

1.4.1. Bitdefender-Symbolleiste

Wenn Ihr Administrator für Security for Endpoints sie eingerichtet hat, informiert Sie die Bitdefender-Symbolleiste über die Sicherheitseinstufung der Webseiten, die Sie ansehen. Die Bitdefender-Symbolleiste ist anders als andere Browser-Symbolleisten. Sie fügt lediglich einen kleinen Dragger zu Ihrem Browser hinzu, der am oberen Rand jeder Webseite angezeigt wird. Mit einem Klick auf den Dragger öffnen Sie die Symbolleiste.

Je nachdem, wie Bitdefender die Webseite einstuft, wird eine der folgenden Nachrichten in der Symbolleiste angezeigt:

- "Diese Seite ist nicht sicher." wird neben einem roten Ausrufezeichen angezeigt.
- "Seien Sie vorsichtig" wird neben einem gelben Ausrufezeichen angezeigt.
- "Diese Seite ist sicher" wird neben einem grünen Häkchen angezeigt.

1.4.2. Suchberater

Falls der Suchberater von Ihrem Security for Endpoints-Administrator eingerichtet wurde, bewertet dieser sowohl die Suchergebnisse von Google, Bing und Yahoo! als auch Links auf Facebook und Twitter, indem es ein Symbol vor jedem Ergebnis anzeigt. Verwendete Symbole und ihre Bedeutung:

Sie sollten diese Webseite nicht aufrufen.

Diese Webseite könnte gefährliche Inhalte haben. Seien Sie vorsichtig, wenn Sie sie dennoch aufrufen möchten.

Diese Seite konnte von Endpoint Security nicht verifiziert werden.

Diese Seite ist sicher.

1.4.3. Gesperrte Webseiten

Abhängig von den von Ihrem Security for Endpoints-Administrator festgelegten Sicherheitsrichtlinien wurden unter Umständen bestimmte Surf-Schutz-Einstellungen eingerichtet, die Phishing-Angriffe und Internet-Betrugsversuche verhindern sollen. Security for Endpoints kann bekannte Phishing-Seiten (Website-Fälschung/Täuschungen) automatisch blockieren, um zu verhindern, dass Sie unbeabsichtigt persönliche oder vertrauliche Informationen an Online-Betrüger weitergeben. Neben gefälschten Webseiten werden auch andere Arten von Online-Bedrohungen unterdrückt, so zum Beispiel Verkaufsbetrug, "Schnelles Geld"-Betrug, Internet-Marketing-Betrug, Klick-Betrug usw. Anstelle der bösartigen Seite wird eine spezielle Warnseite im Browser angezeigt, die Sie darüber informiert, dass die angeforderte Webseite gefährlich ist.



Beachten Sie
Falls Sie eine unbedenkliche Webseite aufrufen möchten, die fälschlicherweise erkannt und blockiert wurde, wenden Sie sich bitte an Ihren Security for Endpoints-Administrator, damit dieser die Seite freigeben kann.

1.5. Geräte-Scan

Endpoint Security kann so konfiguriert werden, dass Speichermedien (CDs/DVDs, USB Speicher oder Netzlaufwerke) automatisch erkannt werden und Sie aufgefordert werden

diese zu scannen oder nicht. Im Warnfenster werden Informationen über das erkannte Gerät angezeigt.

Um das Gerät zu scannen, klicken Sie auf **Ja**. Wenn Sie sicher sind, dass das Gerät sauber ist, können Sie sich entscheiden, es nicht zu scannen.



Beachten Sie
Falls mehrere Geräte gleichzeitig erkannt werden, wird für jedes Gerät nacheinander ein eigenes Warnfenster angezeigt.

Ihr Security for Endpoints-Administrator kann Endpoint Security-Warnungen und -Benachrichtigungen auch unterdrücken. In diesen Fällen wird der Geräte-Scan automatisch gestartet, ohne dass Sie sich darum kümmern müssen.

Wenn ein Geräte-Scan ausgeführt wird, wird ein entsprechendes Symbol für den Scan-Fortschritt in der Task-Leiste angezeigt. Doppelklicken Sie auf dieses Symbol, um das Scan-Fenster zu öffnen und den Scan-Fortschritt anzuzeigen. Sie können den Geräte-Scan jederzeit anhalten oder beenden. Weitere Informationen finden Sie unter „Viren-Scan-Assistent“ (S. 13).

1.6. Anpassen von Schutzeinstellungen

Die Konfiguration und Verwaltung von Endpoint Security erfolgt per Fernzugriff durch Ihren Netzwerkadministrator. Sie können die Schutzeinstellungen nicht bearbeiten.

Sollten Sie Fragen zu Ihren Schutzeinstellungen haben, wenden Sie sich bitte an den für Ihre Netzwerksicherheit verantwortlichen Mitarbeiter.

2. Scannen auf Malware

Die Hauptaufgabe von Endpoint Security ist es, Ihren Computer frei von Malware zu halten. Dies geschieht vornehmlich durch Echtzeit-Scans aller aufgerufenen Dateien, E-Mail-Nachrichten und aller neuen Dateien, die auf Ihren Computer heruntergeladen oder kopiert werden. Neben dem Echtzeitschutz können auch Scans durchgeführt werden, die etwaige Malware auf Ihrem Computer erkennen und entfernen.

Sie können den Computer jederzeit scannen, indem Sie die Standard-Aufgaben oder Ihre eigenen Scan-Aufgaben (benutzerdefinierte Aufgaben) ausführen. Die Scan-Aufgaben beinhalten die Scan-Optionen und die Objekte, die gescannt werden sollen. Wenn Sie bestimmte Bereiche Ihres Computers scannen oder die Scan-Optionen konfigurieren möchten, können Sie einen benutzerdefinierten Scan konfigurieren und ausführen.

2.1. Scannen von Dateien und Ordnern

Wenn Sie den Verdacht hegen, dass Dateien und Verzeichnisse infiziert sein könnten, sollten Sie einen Scan durchführen. Klicken Sie mit der rechten Maustaste auf die Datei oder den Ordner, die/den Sie scannen möchten, und wählen Sie **Mit Endpoint Security von Bitdefender scannen**. Der Viren-Scan-Assistent wird angezeigt. Er führt Sie durch den Scan-Vorgang. Wenn der Scan beendet wurde, werden Sie aufgefordert, die Aktionen auszuwählen, die für die infizierten Dateien ausgeführt werden sollen. Sie können auch entscheiden, keine Aktionen auszuführen.

2.2. Durchführen von Quick Scans

Beim Quick Scan wird das sog In-the-Cloud-Verfahren angewandt, um auf Ihrem System laufende Malware aufzuspüren. Die Ausführung eines Quick Scans dauert im Normalfall weniger als eine Minute und beansprucht nur einen Bruchteil der Systemressourcen, die ein normaler Virenscan in Anspruch nehmen würde.

Um einen Quick Scan auszuführen, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Endpoint Security-Fenster.
2. Gehen Sie zur Tafel **Sicherheit**.
3. Klicken Sie auf **Scan** bei der Option **Quick Scan**.
4. Warten Sie, bis der Viren-Scan-Assistent den Scan abgeschlossen hat. Endpoint Security wird automatisch die empfohlenen Aktionen für die infizierten Dateien ausführen. Sollte es noch ungelöste Bedrohungen geben, werden Sie aufgefordert, die Aktionen auszuwählen, die durchgeführt werden sollen.

2.3. Ausführen eines vollständigen System-Scans

Der vollständige System-Scan scannt den gesamten Computer nach allen Malware-Typen, die ein Sicherheitsrisiko darstellen, so zum Beispiel Viren, Spyware, Adware, Rootkits usw.



Beachten Sie

Da ein **Vollständiger System-Scan** einen gründlichen Scan des gesamten Systems durchführt, kann dieser einige Zeit in Anspruch nehmen. Es empfiehlt sich daher, diese Aufgabe durchzuführen, wenn Sie den Computer nicht benötigen.

Wenn Sie bestimmte Bereiche Ihres Computers scannen oder die Scan-Optionen konfigurieren möchten, können Sie einen benutzerdefinierten Scan konfigurieren und ausführen. Für weitere Informationen lesen Sie bitte „Konfigurieren und Ausführen eines benutzerdefinierten Scans“ (S. 10).

Bevor Sie einen vollständigen System-Scan ausführen, sollten Sie Folgendes beachten:

- Vergewissern Sie sich, dass die Malware-Signaturen von Endpoint Security auf dem neuesten Stand sind. Ihren Computer unter Verwendung einer veralteten Signaturendatenbank zu scannen, kann Endpoint Security daran hindern neue Malware, welche seit dem letzten Update aufkam, zu erkennen. Für weitere Informationen lesen Sie bitte „Updates“ (S. 17).
- Schließen Sie alle geöffneten Programme.

Um einen vollständigen System-Scan durchzuführen, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Endpoint Security-Fenster.
2. Gehen Sie zur Tafel **Sicherheit**.
3. Klicken Sie auf **Scan** bei der Option **Vollständiger Scan**.
4. Warten Sie, bis der Viren-Scan-Assistent den Scan abgeschlossen hat. Endpoint Security wird automatisch die empfohlenen Aktionen für die infizierten Dateien ausführen. Sollte es noch ungelöste Bedrohungen geben, werden Sie aufgefordert, die Aktionen auszuwählen, die durchgeführt werden sollen.

2.4. Konfigurieren und Ausführen eines benutzerdefinierten Scans

Um einen Malware-Scan im Detail zu konfigurieren und dann auszuführen, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Endpoint Security-Fenster.
2. Gehen Sie zur Tafel **Sicherheit**.
3. Klicken Sie auf **Neu** bei der Option **Benutzerdefinierter Scan**.

Ein neues Fenster wird sich öffnen. Folgen Sie diesen Schritten:

a. Sie können die Scan-Optionen einfach durch Einstellen der Scan-Tiefe festlegen. Schieben Sie den Regler dazu in die gewünschte Position. Die Beschreibung auf der rechten Seite der Skala helfen Ihnen, die Scan-Tiefe zu wählen, die für Ihre Bedürfnisse am besten geeignet ist.

   Erfahrene Benutzer können die Scan-Einstellungen von Endpoint Security nutzen. Um die Scan-Optionen im Detail zu konfigurieren, klicken Sie auf **Einstellungen**. Nachdem Sie die gewünschten Einstellungen vorgenommen haben, wird die Scan-Stufe automatisch auf **Benutzerdefiniert** gesetzt. Weitere Informationen zu den benutzerdefinierten Einstellungen finden Sie am Ende dieses Kapitels.

b. Sie können auch folgende allgemeine Optionen konfigurieren:

   - **Aufgabe mit niedriger Priorität ausführen .** Verringert die Priorität des Scan-Vorgangs. Dadurch können andere Programme schneller laufen, der Scan dauert aber länger.
   - **Scan-Assistent in die Task-Leiste minimieren .** Minimiert das Scan-Fenster in die Task-Leiste Es kann durch einen Doppelklick auf das Symbol für den Scan-Fortschritt geöffnet werden.

4. Klicken Sie auf **Weiter**, um die Orte zu wählen, die gescannt werden sollen.
5. Klicken Sie auf die Schaltfläche **Hinzufügen**, um die Orte zu wählen, die gescannt werden sollen. Sie können Sie Liste der Ziele leeren, indem Sie auf die Schaltfläche **Löschen** klicken.
6. Klicken Sie auf **Weiter**, um den Scan zu starten, und warten Sie, bis der Viren-Scan-Assistent den Scan abgeschlossen hat. Abhängig von den Bereichen, die gescannt werden sollen, kann der Scan einige Zeit in Anspruch nehmen. Wenn der Scan beendet wurde, werden Sie aufgefordert, die Aktionen auszuwählen, die für die infizierten Dateien ausgeführt werden sollen. Sie können auch entscheiden, keine Aktionen auszuführen.

Informationen zu den Scan-Optionen

Diese Informationen sind vielleicht nützlich:

- Wenn Ihnen bestimmte Begriffe nicht geläufig sind, schlagen Sie diese im Glossar nach. Sie könne auch durch eine Suche im Internet hilfreiche Informationen finden.
- **Dateitypen.** Sie können Endpoint Security so einstellen, dass alle Dateitypen oder nur Anwendungen (Programmdateien) gescannt werden. Das Scannen aller Dateien bietet den besten Schutz, während das Scannen nur von Anwendungen verwendet wird, um einen schnelleren Scan durchzuführen.

  Anwendungen (oder Programmdateien) sind weitaus anfälliger für Malware-Angriffe als andere Dateitypen. Diese Kategorie beinhaltet die folgenden Dateierweiterungen: `386;`

`a6p; ac; accda; accdb; accdc; accde; accdp; accdr; accdt; accdu; acl; acr; action; ade; adp; air; app; as; asd; asp; awk; bas; bat; bin; cgi; chm; cla; class; cmd; cnv; com; cpl; csc; csh; dat; dek; dld; dll; doc; docm; docx; dot; dotm; dotx; drv; ds; ebm; esh; exe; ezs; fky; frs; fxp; gadget; grv; hlp; hms; hta; htm; html; iaf; icd; ini; inx; ipf; isu; jar; js; jse; jsx; kix; laccdb; lnk; maf; mam; maq; mar; mat; mcr; mda; mdb; mde; mdt; mdw; mem; mhtml; mpp; mpt; mpx; ms; msg; msi; msp; mst; msu; oab; obi; obs; ocx; oft; ole; one; onepkg; ost; ovl; pa; paf; pex; pfd; php; pif; pip; pot; potm; potx; ppa; ppam; pps; ppsm; ppsx; ppt; pptm; pptx; prc; prf; prg; pst; pub; puz; pvd; pwc; py; pyc; pyo; qpx; rbx; rgs; rox; rpj; rtf; scar; scr; script; sct; shb; shs; sldm; sldx; smm; snp; spr; svd; sys; thmx; tlb; tms; u3p; udf; url; vb; vbe; vbs; vbscript; vxd; wbk; wcm; wdm; wiz; wll; wpk; ws; wsf; xar; xl; xla; xlam; xlb; xlc; xll; xlm; xls; xlsb; xlsm; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf; xsn; xtp`

- **Scan-Optionen für Archive.** Archive mit infizierten Dateien sind keine unmittelbare Bedrohung für Ihre Systemsicherheit. Die Malware kann Ihr System nur beeinflussen, wenn die infizierten Datei aus einem Archiv extrahiert und ohne aktivierten Echtzeitschutz ausgeführt wird. Wir empfehlen jedoch, diese Option zu nutzen, um jegliche potentiellen Bedrohungen aufzuspüren und zu entfernen, auch wenn es sich nicht um unmittelbare Bedrohungen handelt.



Beachten Sie
Das Scannen archivierter Dateien erhöht die Gesamt-Scandauer und erfordert mehr Systemressourcen.

- **Boot-Sektoren scannen.** Sie können Endpoint Security einstellen, damit die Boot-Sektoren gescannt werden. Dieser Sektor der Festplatte beinhaltet den notwendigen Computercode um den Boot-Prozess zu starten. Wenn ein Virus den Boot-Sektor infiziert, könnte das Laufwerk unzugänglich werden und es könnte Ihnen nicht mehr möglich sein, Ihr System zu starten und auf Ihre Daten zuzugreifen.
- **Nach Rootkits suchen.** Wählen Sie diese Option, um nach Rootkits und Objekten zu suchen, die mit dieser Art von Software versteckt werden.
- **Speicher scannen.** Wählen Sie diese Option, um Programme zu scannen, die im Speicher Ihres Systems laufen.
- **Registry scannen.** Wählen Sie diese Option, um die Registry-Schlüssel zu scannen. Die Windows-Registry ist eine Datenbank, in der Konfigurationseinstellungen und Optionen für die Windows-Betriebssystemkomponenten sowie für die installierten Anwendungen gespeichert sind.

- **Cookies scannen.** Wählen Sie diese Option, um die Cookies zu scannen, die von Ihrem Browser auf Ihrem Computer gespeichert werden.
- **Nur neue und geänderte Dateien.** Indem nur neue und geänderte Dateien gescannt werden, können Sie die allgemeine Systemreaktionsfähigkeit mit minimalen Sicherheitsabstrichen erheblich verbessern.
- **Kommerzielle Keylogger ignorieren.** Wählen Sie diese Option, wenn Sie auf Ihrem Computer eine kommerzielle Keylogger-Software nutzen. Kommerzielle Keylogger sind seriöse Programme zur Überwachung des Computers, deren Hauptfunktion es ist, alle Tastatureingaben aufzuzeichnen.

2.5. Viren-Scan-Assistent

Der Endpoint Security-Viren-Scan-Assistent erscheint, sobald Sie einen Bedarf-Scan starten (zum Beispiel, indem Sie mit der rechten Maustaste auf einen Ordner klicken und dann **Mit Endpoint Security von Bitdefender scannen** auswählen). Folgen Sie den Anweisungen des Assistenten, um den Scan-Prozess abzuschließen.



Beachten Sie

Falls der Scan-Assistent nicht erscheint, ist der Scan möglicherweise konfiguriert, im Hintergrund zu laufen. Achten Sie auf das Symbol B für den Scan-Fortschritt in der Task-Leiste. Doppelklicken Sie auf dieses Symbol, um das Scan-Fenster zu öffnen und den Scan-Fortschritt anzuzeigen.

2.5.1. Schritt 1 - Führen Sie den Scan durch

Endpoint Security startet den Scan der aus gewählten Dateien und Verzeichnisse. Sie erhalten Echtzeitinformationen über den Scan-Status sowie Scan-Statistiken (einschließlich der bisherigen Laufzeit, einer Einschätzung der verbleibenden Laufzeit und der Anzahl der erkannten Bedrohungen). Klicken Sie auf **Mehr anzeigen**, um weitere Details zu erhalten.

Bitte warten Sie, bis der Scan abgeschlossen ist. Der Scan-Vorgang kann, abhängig von der Größe Ihrer Festplatte, eine Weile dauern.

Einen Scan anhalten oder unterbrechen. Sie können den Scan-Vorgang jederzeit durch einen Klick auf **Abbrechen** abbrechen. Sie gelangen dann direkt zum letzten Schritt des Assistenten. Um den Scan-Vorgang vorübergehend anzuhalten, klicken Sie einfach auf **Pause**. Um den Scan-Vorgang fortzusetzen klicken Sie auf **Fortsetzen** .

Passwortgeschützte Archive. Wird ein passwortgeschütztes Archiv gefunden, werden Sie, abhängig von den Scan-Einstellungen, um die Eingabe des Passwortes gebeten. Mit Passwort geschützte Archive können nicht gescannt werden, außer wenn Sie das Passwort angeben. Die folgenden Optionen sind verfügbar:

- **Passwort.** Wenn Sie möchten, dass Endpoint Security Archive scannt, wählen Sie diese Option aus und geben das Passwort an. Falls Sie das Passwort nicht kennen, wählen Sie eine der anderen Optionen.
- **Nicht nach Passwort fragen; das Objekt beim Scan überspringen.** Wählen Sie diese Option um das Scannen diesen Archivs zu überspringen.
- **Alle passwortgeschützte Dateien überspringen ohne diese zu scannen.** Wählen Sie diese Option, falls Sie nicht über passwortgeschützte Archive informiert werden möchten. Endpoint Security kann diese Dateien und Objekte nicht scannen, erstellt aber einen Eintrag im Scan-Protokoll.

Wählen Sie die gewünschte Option aus und klicken Sie auf **OK**, um den Scan fortzusetzen.

2.5.2. Schritt 2 - Wählen Sie entsprechende Aktionen aus

Wenn der Scan beendet wurde, werden Sie aufgefordert, die Aktionen auszuwählen, die für die infizierten Dateien ausgeführt werden sollen. Sie können auch entscheiden, keine Aktionen auszuführen.



Beachten Sie

Wenn Sie einen Quick Scan oder einen vollständigen System-Scan durchführen, wird Endpoint Security während des Scans automatisch die empfohlenen Aktionen für die infizierten Dateien ausführen. Sollte es noch ungelöste Bedrohungen geben, werden Sie aufgefordert, die Aktionen auszuwählen, die durchgeführt werden sollen.

Die infizierten Objekte werden in Gruppen angezeigt, je nach Malware, mit der sie infiziert sind. Klicken Sie auf den Link, der der Bedrohung entspricht, um weitere Informationen über die infizierten Objekte zu erhalten.

Sie können eine umfassende Aktion für alle Probleme auswählen oder Sie können einzelne Aktionen für Problemgruppen auswählen. Eine oder mehrere der folgenden Optionen können im Menu erscheinen:

Aktionen ausführen

Endpoint Security wird je nach Art der infizierten Datei die empfohlenen Aktionen ausführen:

- **Infizierte Dateien.** Als infiziert eingestufte Dateien stimmen mit einer Malware-Signatur der Bitdefender Malware-Signaturen-Datenbank überein. Endpoint Security wird automatisch versuchen, den Malware-Code aus der infizierten Datei zu entfernen und die Originaldatei zu rekonstruieren. Diese Operation bezeichnet man als Desinfektion.

  Dateien, die nicht desinfiziert werden können, werden in die Quarantäne verschoben, um so die Infizierung einzudämmen. Dateien in der Quarantäne können nicht ausgeführt oder geöffnet werden; aus diesem Grund besteht kein Infektionsrisiko.



Wichtig
Bestimmte Malware-Typen können nicht desinfiziert werden, da die komplette Datei betroffen ist. In diesen Fällen wird die infizierte Datei von der Festplatte gelöscht.

- **Verdächtige Dateien.** Dateien werden von der heuristischen Analyse als verdächtig klassifiziert. Verdächtige Dateien können nicht desinfiziert werden, da hierfür keine Desinfektionsroutine verfügbar ist. Sie werden in Quarantäne verschoben, um eine mögliche Infektion zu verhindern.

  Dateien in Quarantäne werden standardmäßig an die Bitdefender-Labore geschickt, damit Sie dort von den Bitdefender-Malware-Forschern analysiert werden können. Sollten das Vorhandensein von Malware bestätigt werden, wird eine Signatur veröffentlicht, um das Entfernen der Malware zu ermöglichen.
- **Archive mit infizierten Dateien.**
  - Archive, die nur infizierte Dateien enthalten, werden automatisch gelöscht.
  - Wenn ein Archiv sowohl infizierte als auch nicht infizierte Dateien enthält, wird Endpoint Security versuchen, die infizierten Dateien zu löschen, vorausgesetzt, dass das Archiv mit den nicht infizierten Dateien wieder rekonstruiert werden kann. Wenn das Archiv nicht rekonstruiert werden kann, werden Sie benachrichtigt, dass keine Aktion durchgeführt werden kann, weil die Gefahr besteht, dass nicht infizierte Dateien verloren gehen.

Löschen
Infizierte Dateien werden von der Festplatte entfernt.

Falls infizierte Dateien zusammen mit nicht infizierten Dateien in einem Archiv gespeichert sind, wird Endpoint Security versuchen, die infizierten Dateien zu löschen und das Archiv mit den nicht infizierten Dateien zu rekonstruieren. Wenn das Archiv nicht rekonstruiert werden kann, werden Sie benachrichtigt, dass keine Aktion durchgeführt werden kann, weil die Gefahr besteht, dass nicht infizierte Dateien verloren gehen.

Ignorieren
Es wird keine Aktion für die infizierte Dateien ausgeführt. Nachdem der Scan-Vorgang beendet wurde, können Sie das Scan-Protokoll öffnen um Informationen über diese Dateien anzuzeigen.

Klicken Sie auf **Fortfahren** um die festgelegten Aktionen anzuwenden.

2.5.3. Schritt 3 - Zusammenfassung

Wenn Endpoint Security die Probleme gelöst hat, wird eine Zusammenfassung der Scan-Ergebnisse in einem neuen Fenster angezeigt. Falls Sie umfangreichere Informationen zum Scan-Prozess möchten, klicken Sie auf **Logdatei anzeigen**.

Klicken Sie auf **Schließen** um dieses Fenster zu schließen.



Wichtig

In den meisten Fällen desinfiziert Endpoint Security erfolgreich die aufgespürten infizierten Dateien oder er isoliert die Infektion. Dennoch gibt es Probleme, die nicht automatisch gelöst werden können. Bitte starten Sie Ihr System neu, wenn Sie dazu aufgefordert werden, damit der Säuberungsprozess abgeschlossen werden kann.

2.6. Scan-Protokolle werden überprüft

Für jeden Scan wird ein Protokoll erstellt. Der Bericht enthält detaillierte Informationen über den Scan-Vorgang, so wie Scan-Optionen, das Scan-Ziel, die gefundenen Bedrohungen und die Aktionen, die für diese Bedrohungen ausgeführt wurden.

Sobald der Scan beendet ist, können Sie das Scan-Protokoll direkt aus dem Scan-Assistenten heraus öffnen, indem Sie auf **Protokoll anzeigen** klicken.

Um die Scan-Protokolle zu einem späteren Zeitpunkt zu überprüfen, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Endpoint Security-Fenster.
2. Gehen Sie zur Tafel **Ereignisse**.
3. Wählen Sie **Malware-Schutz** im zweiten Menü. Hier können Sie alle Malware-Scan-Ereignisse finden, einschließlich der Bedrohungen, die während Zugriff-Scans und vom Benutzer gestarteten Scans entdeckt wurden. Dazu kommen Statusänderungen für automatische Scans.
4. In der Ereignisliste können Sie überprüfen, welche Scans kürzlich durchgeführt wurden. Klicken Sie auf ein Ereignis, um mehr darüber zu erfahren.
5. Sie können das Scan-Protokoll öffnen, indem Sie auf den Ort klicken, der im Detailbereich unten auf der Tafel angegeben ist. Das Scan-Protokoll wird angezeigt.

3. Updates

In einer Welt, in der Internet-Kriminelle immer neue Wege finden, um Ihnen zu schaden, ist es von größter Wichtigkeit, dass Sie Ihre Sicherheitslösung zu jeder Zeit auf dem neuesten Stand halten, um stets einen Schritt voraus zu sein.

Falls Sie über eine Breitbandverbindung oder eine DSL-Verbindung verfügen, arbeitet Endpoint Security eigenständig. Standardmäßig sucht die Software nach Updates, wenn Sie Ihren Computer einschalten und danach einmal pro **Stunde**. Wenn ein neues Update erkannt wird, wird es automatisch auf Ihren PC heruntergeladen und installiert.



Beachten Sie

Die standardmäßige Frequenz für automatische Updates kann von Ihrem Netzwerkadministrator angepasst werden. Für weitere Informationen lesen Sie bitte „Wobei handelt es sich bei der Frequenz für automatische Updates?“ (S. 18).

Der Updatevorgang wird "on the fly" durchgeführt, das bedeutet die entsprechenden Dateien stufenweise aktualisiert werden. So stört der Update-Vorgang nicht den Betrieb des Produkts, während gleichzeitig alle Schwachstellen behoben werden.

Falls Sie sich per Einwahl mit dem Internet verbinden, ist es sinnvoll, regelmäßig ein manuelles Bitdefender-Update durchzuführen. Für weitere Informationen lesen Sie bitte „Durchführung eines Updates“ (S. 18).

3.1. Arten von Updates

Folgende Update-Möglichkeiten stehen zur Verfügung:

- **Updates der Malware-Signaturen** - Immer wenn neue Bedrohungen auftreten, müssen die Dateien mit den Malware-Signaturen aktualisiert werden, um einen durchgängigen und aktuellen Schutz zu gewährleisten.
- **Produkt-Updates** - wenn eine neue Version auf dem Markt erscheint, enthält diese zur Leistungssteigerung des Produkts neue Funktionen und Scantechniken.

  Bei einem Produkt-Upgrade handelt es sich um eine neue Hauptversion der Software.

3.2. Überprüft, ob Ihr Schutz auf dem neuesten Stand ist

Um zu überprüfen, ob Ihr Schutz auf dem neuesten Stand ist, gehen Sie folgendermaßen vor:

1. Klicken Sie mit der rechten Maustaste auf das Endpoint Security-Symbol in der Task-Leiste und wählen Sie danach **Über**.
2. Der Update-Status und der Zeitpunkt der letzten Update-Überprüfung und Update-Installation werden angezeigt.

Um ausführliche Informationen zu Ihren letzten Updates zu erhalten, rufen Sie die Update-Ereignisse auf:

1. Gehen Sie im Hauptfenster zur Tafel **Ereignisse**.
2. Klicken Sie im zweiten Menü auf **Update**.

Sie können herausfinden, wann Updates angestoßen wurden und weitere Informationen dazu einholen (d.h. ob sie erfolgreich waren oder nicht, ob ein Neustart erforderlich ist, um die Installation abzuschließen). Falls nötig starten Sie das System sobald es Ihnen möglich ist neu.

3.3. Durchführung eines Updates

Sie benötigen eine Internet-Verbindung, um Updates durchzuführen.

Um ein Update zu starten, klicken Sie mit der rechten Maustaste auf das Endpoint Security-Symbol in der Task-Leiste und wählen Sie **Über**. Wenn Sie das **Über**-Fenster öffnen, wird dadurch automatisch ein Bedarf-Update gestartet.

Das Update-Modul verbindet sich mit dem Bitdefender-Update-Server und sucht nach verfügbaren Updates. Wenn ein neues Update erkannt wird, wird es automatisch auf Ihren PC heruntergeladen und installiert.



Wichtig
Möglicherweise kann ein Neustart nach dem vollständig durchgeführten Update notwendig werden. Wir empfehlen, das so bald wie möglich zu tun.

3.4. Wobei handelt es sich bei der Frequenz für automatische Updates?

Endpoint Security sucht automatisch nach Updates, wenn Sie Ihren Computer einschalten und dann jede **Stunde** danach erneut.

4. Ereignisanzeige

Endpoint Security führt ein detailliertes Ereignisprotokoll über alle Aktivitäten der Software auf Ihrem Computer (einschließlich der Computer-Aktivitäten, die von der Inhaltssteuerung überwacht werden). Ereignisse sind ein wichtiges Hilfsmittel für die Überwachung Ihres Bitdefender-Schutzes. So können Sie beispielsweise einfach überprüfen ob das Update erfolgreich durchgeführt wurde, ob Malware auf Ihrem entdeckt wurde usw.

Um das Ereignisprotokoll aufzurufen, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Endpoint Security-Fenster.
2. Gehen Sie zur Tafel **Ereignisse**.
3. Wählen Sie im zweiten Menü die Ereigniskategorie aus. Ereignisse sind in die folgenden Kategorien unterteilt:
   - **Malware-Schutz**
   - **Inhaltssteuerung**
   - **Update**
   - **Firewall**
   - **Allgemein**

Eine Liste von Ereignissen ist für jede Kategorie verfügbar. Um weitere Informationen über ein bestimmtes Ereignis in der Liste zu erhalten, müssen Sie nur darauf klicken. Details zu dem Ereignis werden in der unteren Hälfte des Fensters angezeigt. Sie erhalten die folgenden Informationen zu jedem Ereignis: eine Kurzbeschreibung; die Aktion, die Bitdefender für beim Auftreten des Ereignisses durchgeführt hat; das Datum und der Zeitpunkt des Ereignisses.

Sie können Ereignisse nach Ihrer Dringlichkeit ordnen. Es gibt drei Ereignistypen:

Information Diese Ereignisse weisen auf erfolgreich ausgeführte Vorgänge hin.

Warnung Diese Ereignisse weisen auf nicht-kritische Probleme hin.

Kritische Ereignisse weisen auf kritische Probleme hin.

Ereignisse können nur von Ihrem Netzwerkadministrator gelöscht werden.

5. Hilfe erhalten

Sollten Sie Probleme oder Fragen zu Endpoint Security haben, wenden Sie sich bitte an Ihren Netzwerkadministrator.

Um Produkt- und Kontaktinformationen zu finden, können Sie folgendermaßen vorgehen:

- Öffnen Sie das Endpoint Security-Fenster und klicken Sie in der unteren rechten Bildschirmecke auf das **Info**-Symbol.
- Klicken Sie mit der rechten Maustaste auf das Endpoint Security-Symbol in der Task-Leiste und wählen Sie danach **Über**.

Glossar

Adware

Adware wird häufig mit einer anderen Anwendung kombiniert, die kostenlos ist, solange der Nutzer die Adware akzeptiert. Adware-Anwendungen werden in der Regel installiert, nachdem der Nutzer einer Lizenzvereinbarung zugestimmt hat. In der Lizenzvereinbarung wird auch der Zweck der Anwendung genannt, und somit liegt keine Rechtswidrigkeit vor.

Allerdings können Popup-Anzeigen mit der Zeit sehr lästig werden und in manchen Fällen die Systemperformance beeinträchtigen. Zudem kann aufgrund der Daten, die manche dieser Programme sammeln, die Privatsphäre von Nutzern verletzt werden, die sich über die Bedingungen in der Lizenzvereinbarung nicht völlig im Klaren waren.

Antivirus-Storm

Eine intensive Beanspruchung von Systemressourcen, die auftritt, wenn Virenschutz-Software gleichzeitig mehrere virtuelle Maschinen auf einem einzigen physischen Host scannt.

Archive

Ein Datenträger, ein Magnetband oder ein Ordner mit Dateien, die von einem Backup erzeugt wurden.

Eine Datei, die eine oder mehrere Dateien in einem komprimierten Format enthält.

Backdoor (Hintertür)

Eine Sicherheitslücke eines Systems, die der Entwickler oder Administrator absichtlich hinterlässt. Der Grund dafür muss nicht immer bösartig sein. Manche Betriebssysteme haben schon standardmäßig privilegierte Konten eingerichtet, damit diese von den Kundendienst-Technikern oder Programmierern der Hersteller benutzt werden können.

Befehlszeile

Die Befehlszeile ist eine zeichenorientierte Benutzerschnittstelle. Die Kommunikation zwischen Benutzer und Computer findet ausschließlich durch die Eingabe von bestimmten Befehlen statt, die sich aus einzelnen Buchstabenfolgen zusammensetzen. Als Eingabegerät wird eine Tastatur benutzt. Die Verwendung einer Maus ist nicht möglich. Auf der Befehlszeile werden die einzelnen Anweisungen in einer bestimmten Befehlssprache eingegeben, die vom Computer und seiner Software ausgewertet und mit den entsprechenden Ergebnissen auf dem Ausgabegerät (meistens ein Monitor) wieder an den Benutzer übergeben werden.

Bootsektor

Der erste Sektor einer Festplatte oder Diskette. Hier liegen Daten, die das Betriebssystem zum Booten (Starten) braucht.

Bootvirus

Ein Virus, der den Bootsektor einer Festplatte oder eines Diskettenlaufwerks infiziert. Beim Versuch von einer Diskette, die mit einem Bootvirus infiziert ist, zu booten wird dieser im Arbeitsspeicher aktiviert. Bei jedem Neustart wird der Virus so im Arbeitsspeicher aktiviert und überträgt sich auf eingelegte Wechselmedien.

Cookie

In der Internetbranche werden mit Cookies kleine Dateien bezeichnet, die Daten über einzelne Computer enthalten und die von den Werbetreibenden analysiert und verwendet werden, um die Interessen und Vorlieben der Benutzer herauszufinden. Die Cookie-Technologie wird stetig weiterentwickelt mit dem Ziel Benutzern nur noch solche Werbung anzuzeigen, die ihren Interessen entspricht. Für viele ist dies ein zweischneidiges Schwert. Einerseits ist es praktisch, nur Anzeigen zu sehen, an denen man interessiert ist. Anderseits bedeutet es, dass Online-Aktivitäten der Benutzer gewissermaßen auf Schritt und "Klick" verfolgt werden. Es ist also verständlich, dass in diesem Zusammenhang Datenschutz ein umstrittenes Thema ist und viele sich unwohl fühlen, quasi als SKU-Nummer (die Strichcodes auf den Packungen, die im Geschäft an der Theke gescannt werden) betrachtet zu werden. Auch wenn diese Sicht etwas extrem erscheint, ist sie doch manchmal korrekt.

Dateierweiterung

Der Teil hinter dem Punkt im Dateinamen. Die Erweiterung oder Extension beschreibt die Art der Daten, die in einer Datei gespeichert sind.

Viele Betriebssysteme benutzen Dateierweiterungen, z.B. Unix, VMS, MS-DOS. Sie sind gewöhnlich ein bis drei Buchstaben lange (alte Betriebssysteme können oft nicht mehr als drei Buchstaben unterstützen). Beispiele sind "exe" ausführbare Dateien, "ps" für PostScript oder "txt" für Text-Dateien.

Durchsuchen

Kurzform für Web-Browser, ein Programm, mit dem Internetseiten aufgerufen und angezeigt werden können. Die bekanntesten Browser sind Mozilla Firefox und Microsoft Internet Explorer. Beide sind graphische Browser, was bedeutet, dass sie sowohl Grafiken als auch Texte anzeigen können. Weiterhin können die meisten Browser Multimedia-Daten wie Klang- und Videodateien anzeigen, wobei sie für diverse Formate Plug-Ins (zusätzliche Softwarekomponenten) benutzen.

Ereignisanzeige

Ereignisse oder Erscheinungen, die in einem Programm vorkommen. Ereignisse können Benutzeraktionen, wie zum Beispiel Mausklicks oder Tastatureingaben, oder Systemereignisse, wie zum Beispiel ungenügender Speicher, sein.

Fehlalarm

Erscheint, wenn ein Virenscanner eine Datei als infiziert erkennt, obwohl dies nicht der Fall ist.

Heuristik

Eine Methode, um neue Viren zu identifizieren. Diese Scan-Methode benötigt keine spezifischen Virussignaturen. Der Vorteil eines heuristischen Scans ist, dass man nicht von einer neuen Variante eines alten Virus getäuscht werden kann. Manchmal kann jedoch auch ein verdächtiger Code in einem normalen Programm gemeldet werden, ein sogenannter Fehlalarm oder "falsch-positive Meldung" wird angezeigt.

IP

Internet Protocol - Das TCP/IP Protokoll ist verantwortlich für die korrekte IP Adressierung und die korrekte Zustellung der Datenpakete.

Keylogger

Ein Keylogger ist eine Anwendung, die alles aufzeichnet, was Sie tippen.

Keylogger sind an sich nicht schädlich. Sie können auch legitim eingesetzt werden, um beispielsweise die Aktivitäten von Angestellten oder Kindern zu überwachen. Sie werden jedoch zunehmend von Cyber-Kriminellen mit bösartiger Absicht eingesetzt (um beispielsweise private Daten wie Benutzernamen oder Passwörter zu sammeln).

Logdatei (Berichtsdatei)

Eine Datei, die stattgefundene Aktivitäten aufzeichnet. Zum Beispiel speichert Bitdefender eine Prokolldatei mit den gescannten Pfaden, Ordnern, der Anzahl der gescannten Archive und Dateien sowie der Anzahl der gefundenen infizierten oder verdächtigen Dateien.

Makrovirus

Eine Virusform, die in einem Dokument als eingebettetes Makro verschlüsselt wird. Viele Anwendungen, wie Microsoft Word und Excel, unterstützen leistungsstarke Makrosprachen.

Diese Anwendungen ermöglichen das Einbetten eines Makros in ein Dokument, welches dann bei jedem Öffnen des Dokuments ausgeführt wird.Ein Makro ist eine Aufzeichnung des Ablaufs von Routineaufgaben innerhalb des makrofähigen Programms, das dann immer wieder verwendet werden kann.

Malware

Malware ist der Sammelbegriff für alle Software-Arten, die darauf ausgelegt sind, Schaden zu verursachen - das Wort setzt sich zusammen aus den englischen Begriffen malicious und software, also bösartige Software. Der Begriff hat sich noch nicht vollständig durchgesetzt, wird aber immer häufiger als Oberbegriff gebraucht, wenn von Viren, Trojanern, Würmern und Malicious Mobile Code die Rede ist.

Malware-Signatur

Malware-Signaturen sind Codebruchstücke, die aus aktuellen Malware-Beispielen extrahiert werden. Diese werden von Antiviren-Programmen zum Musterabgleich und zur Aufspürung von Malware verwendet. Signaturen werden auch genutzt, um den Malware-Code aus infizierten Dateien zu entfernen.
Die Bitdefender Malware-Signatur-Datenbank ist eine Sammlung von stündlich durch Bitdefender-Mitarbeiter upgedateten Malware-Signaturen.

Nicht heuristisch

Diese Scan-Methode beruht auf spezifischen Virussignaturen. Der Vorteil eines nicht-heuristischen Scans ist, dass er nicht von einem Scheinvirus getäuscht werden kann und so Fehlalarme verhindert.

Phishing

Das Senden einer E-Mail an einen Benutzer, in der der Sender sich als Vertreter eines legitimen Unternehmens ausgibt und versucht, den Empfänger so zu manipulieren, dass er persönliche Informationen preisgibt, die dann zum Diebstahl der Identität verwendet werden können. Die E-Mail leitet den Benutzer dann auf eine Webseite, auf der er aufgefordert wird, vertrauliche Daten wie Kreditkartennummern, TANs oder PINs preiszugeben. Es wird oft vorgegeben, dass dies aus Gründen der Aktualisierung geschehen soll. Diese Webseiten sind jedoch gefälscht und wurden eigens für den Diebstahl dieser Daten eingerichtet.

Polymorpher Virus

Ein Virus, der seine Form mit jeder Datei, die er infiziert, ändert. Da diese Viren kein beständiges binäres Muster haben, sind sie sehr schwer zu erkennen.

Rootkit

Bei einem Rootkit handelt es sich um eine Sammlung von Software-Tools, mit denen auf ein System mit Administratorrechten zugegriffen werden kann. Der Begriff wurde ursprünglich nur für UNIX-Systeme verwendet und beschrieb rekompilierte Tools, mit denen sich Angreifer Administratorrechte verschaffen und so ihre Anwesenheit vor den tatsächlichen Administratoren verbergen konnten.

Die Hauptaufgabe eines Rootkits besteht darin, Prozesse, Dateien und Protokolle zu verstecken. Sie können auch Daten von Terminals, Netzwerkverbindungen oder Peripheriegeräten abfangen, falls Sie eine entsprechende Software eingebaut haben.

Rootkits sind nicht grundsätzlich schädlich. Einige Systeme und Anwendungen verstecken z. B. wichtige Dateien mithilfe von Rootkits. Sie werden jedoch oft dazu missbraucht, Malware zu verbergen oder unbemerkt einen Eindringling einzuschleusen. In Kombination mit Malware stellen sie eine große Gefahr für Ihr System dar. Denn sie können den Datenverkehr abhören, Sicherheitslücken in Ihrem System schaffen, Dateien und Zugangsdaten verändern, und das alles, ohne entdeckt zu werden.

Schnittstelle

Stelle eines Rechners, an die ein Gerät angeschlossen werden kann. Rechner haben verschiedenartige Schnittstellen. Im Inneren gibt es Schnittstellen zum Anschluss von Festplatten, Grafikkarten und Tastaturen. Extern haben Rechner Schnittstellen zum Anschluss von Modems, Druckern und anderen Peripheriegeräten.

In TCP/IP und UDP Netzwerken, ein Endpunkt zu logischen Verbindungen. Die Schnittstellennummer gibt die Art der Schnittstelle an. Zum Beispiel, Schnittstelle 80 wird für HTTP Traffic verwendet.

Script

Ein anderer Begriff für Makro- oder Batchdatei. Ein Skript ist eine Befehlsliste, die ohne Benutzereingriff ausgeführt werden kann.

Spam

Junk-E-Mail oder Junk-Postings in Newsgroups. Im Allgemeinen versteht man darunter jede Art von unerwünschter E-Mail.

Spyware

Software, die unentdeckt vom Nutzer private und geheime Anwenderdaten über seine Internetverbindung abgreift. Dies geschieht in der Regel zu Werbezwecken. Typischerweise sind Spyware-Anwendungen als verborgene Komponenten in Freeware- oder Shareware-Programmen enthalten, die aus dem Internet heruntergeladen werden können. Die große Mehrzahl von Shareware- und Freeware-Anwendungen ist natürlich frei von Spyware. Ist die Spyware einmal installiert, überwacht sie die Nutzeraktivitäten und überträgt diese Daten im Hintergrund an einen Dritten. Spyware kann auch Informationen über E-Mail-Adressen und sogar Passwörter und Kreditkartennummern sammeln.

Einem Trojanischen Pferd ähnelt Spyware darin, dass die Anwender das Produkt unwissentlich gemeinsam mit etwas anderem installieren. Opfer von Spyware wird man oft dann, wenn man sich bestimmte Peer-to-Peer-Dateiaustauschprogramme herunterlädt.

Ganz abgesehen von den Fragen der Ethik und des Datenschutzes belegt Spyware auch unnötig Systemressourcen und Bandbreite, indem über die Internetverbindung des Nutzers Informationen an den Spyware-Heimatserver gesendet werden. Da Spyware Speicher und Systemressourcen verbraucht, können die im Hintergrund laufenden Anwendungen zu Systemabstürzen oder allgemeiner Systeminstabilität führen.

Symbolleiste

Die Symbolleiste wurde mit Windows 95 eingeführt und befindet sich auf der Windows Task-Leiste (gewöhnlich unten rechts, dort wo sich auch die Uhrzeit befindet). Sie enthält kleine Symbole zur Information und zum leichteren Zugriff auf Systemfunktionen wie Drucker, Modems, Lautstärke und anderes. Um auf die Details und Optionen dieser

Funktionen zuzugreifen, ist ein Doppelklick oder ein Klick mit der rechten Maustaste erforderlich.

TCP/IP

Transmission Control Protocol/Internet Protocol – im Internet weit verbreiteter Netzwerkprotokollsatz, der die Kommunikation zwischen verbundenen Computernetzwerken mit verschiedenen Hardware-Architekturen und Betriebssystemen ermöglicht. TCP/IP bietet eine Möglichkeit, all diese unterschiedlichen Komponenten zu Kommunikationszwecken miteinander zu verbinden.

Trojaner

Ein bösartiges Programm, das sich als eine legitime Anwendung ausgibt. Im Unterschied zu Viren vervielfältigen sich die Trojaner (auch "trojanische Pferde" genannt) nicht, aber sie können ebenso schädlich sein. Einer der heimtückischsten Trojaner ist ein Programm, das behauptet Ihren Rechner von Viren zu befreien, stattdessen aber den Rechner infiziert.

Der Begriff entstammt einer Geschichte in Homers "Ilias", in der die Griechen ihren Feinden, den Trojanern, angeblich als Sühnegabe ein riesiges hölzernes Pferd schenkten. Aber nachdem die Trojaner das Pferd in die Stadt gebracht hatten, schlichen sich die im Bauch des hölzernen Pferdes versteckten Soldaten bei Nacht heraus, öffneten die Tore der Stadt und ermöglichten somit ihren Landsleuten, in die Stadt einzudringen und auf diese Weise Troja zu besetzen.

Update

Eine neue Software- oder Hardwareversion, die eine ältere Version desselben Produkts ersetzt. Die Update-Installationsroutine eines Programms prüft oft, ob eine ältere Versionen auf dem Rechner installiert ist, da sonst kein Update installiert werden kann.

Bitdefender verfügt über ein eigenes Update-Modul, das die manuelle oder automatische Suche nach Updates ermöglicht.

Virus

Ein Programm oder ein Stück Code, das auf einen Rechner kopiert wird und sich allein ausführt, ohne dass es der Besitzer des Rechners will oder merkt. Die meisten Viren können sich auch selbst vervielfältigen. Alle Computerviren wurden von Menschen programmiert. Ein Virus, der sich immer wieder vervielfältigen kann, ist sehr einfach zu programmieren. Sogar ein solch einfacher Virus kann gefährlich sein, da er im Handumdrehen sämtlichen Arbeitsspeicher belegen und so das System lahmlegen kann. Noch gefährlicher sind Viren, die sich über Netzwerke selbst weiterversenden und Sicherheitssysteme umgehen.

Wurm

Ein Programm, das sich selbst kopiert und über ein Netzwerk verbreitet. Es kann sich nicht an andere Programme anhängen.